

10/069118

PCT/JP00/05832

日本国特許庁

13.09.00

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年 8月30日

REC'D 06 NOV 2000

WIPO

PCT

出願番号
Application Number:

平成11年特許願第243583号

出願人
Applicant(s):

富士通株式会社
日本コロムビア株式会社
三洋電機株式会社

JP00/05832

4

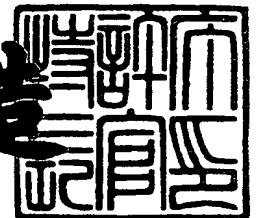
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3085321

【書類名】 特許願
 【整理番号】 1990903
 【提出日】 平成11年 8月30日
 【あて先】 特許庁長官殿
 【国際特許分類】 H04M 11/08

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 畑中 正行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 蒲田 順

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 畠山 卓久

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 長谷部 高行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社
社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社
社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社
社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ再生装置

【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第 1 の復号鍵を保持する第 1 の鍵保持部と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第 1 の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第 1 の復号処理部と、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第 1 の復号処理部の出力により復号してコンテンツデータを抽出するための第 2 の復号処理部を含む、データ再生装置。

【請求項 2】 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第 1 のセッションキーを生成する第 1 のセッションキー発生部と、

前記第 1 のセッションキーを前記データ格納部にて復号可能な第 1 の暗号鍵で暗号化して前記データ格納部に与えるための第 1 の暗号化処理部と、

前記第 1 のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第 1 のセッションキーについて復号して前記第 1 の復号処理部に与える第 3 の復号処理部をさらに含む、請求項 1 記載のデータ再生装置。

【請求項 3】 前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第 2 のセッションキーを、さらに、前記第 1 の復号鍵により復号可能な暗号化を施して供給を受け、前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第 1 のセッションキーを生成する第 1 のセッションキー発生部と、

前記第 1 のセッションキーを、外部から入力されたデータから前記第 1 の複合鍵に基づいて前記第 1 の復号処理部にて抽出された前記第 2 のセッションキーで暗号化して前記データ格納部に与えるための第 2 の暗号処理部と、

前記第 1 のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第 1 のセッションキーについて復号して前記第 1 の復号処理部に与える第 3 の復号処理部をさらに含む、請求項 1 記載のデータ再生装置。

【請求項 4】 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項 1 ～ 3 のいずれか 1 項に記載のデータ再生装置。

【請求項 5】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記憶部と、

前記第 1 の暗号化鍵を保持する第 2 の鍵保持部と、

前記第 1 の暗号化鍵により暗号化されたデータを復号するための第 2 の復号鍵を保持するための第 3 の鍵保持部と、

前記第 2 の復号鍵に基づいて、前記データ再生部から前記第 1 の暗号化鍵により暗号化されて伝達された前記第 1 のセッションキーを復号するための第 4 の復号処理部と、

前記第 4 の復号処理部で抽出された前記第 1 のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第 2 の暗号化処理部を備える、請求項 2 記載のデータ再生装置。

【請求項 6】 前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記録部と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第 2 のセッションキーを発生する第 2 のセッションキー発生部と、

前記第 1 の復号鍵にて復号可能な第 2 の暗号化鍵により、暗号化処理を行なう第 3 の暗号化処理部と、

前記第 2 のセッションキーに基づいて、前記データ再生部から前記第 2 のセッションキーにて暗号化されて伝達された前記第 1 のセッションキーを復号するための第 5 の復号処理手段と、

前記第 5 の復号処理手段にて抽出された前記第 1 のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第 4 の暗号化処理部を備える、請求項 3 記載のデータ再生装置。

【請求項 7】 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項 5 または 6 記載のデータ再生装置。

【請求項 8】 前記データ再生部は、

少なくとも前記第 1 の鍵保持部と、前記第 1 の復号処理部と、前記第 2 の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項 1 記載のデータ再生装置。

【請求項 9】 前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項 1 ～ 4 のいずれか 1 項に記載のデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0 0 0 4】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0 0 0 6】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権情報の配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

【0 0 0 7】

このような記録装置としては、たとえば、メモ리카ードのように電氣的にデータの書込および消去が可能な媒体が用いられることになる。

【0 0 0 8】

さらに、配信データを再生する装置としては、このようなデータの配信を受け

るのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

【0009】

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティー対策を施す必要がある。

【0010】

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができる」とすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来すことになる。

【0011】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

【0012】

【課題を解決するための手段】

請求項1記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツキーを復号するための第1の復号鍵を保持する第1の鍵保持部と、データ格納部からの暗号

化コンテンツキーを基にして、第1の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する第1の復号処理部と、データ格納部から読み出された暗号化コンテンツデータを受けて、第1の復号処理部の出力により復号してコンテンツデータを抽出するための第2の復号処理部を含む。

【0013】

請求項2記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスする毎に更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーをデータ格納部に復号可能な第1の暗号鍵で暗号化してデータ格納部に与えるための第1の暗号化処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

【0014】

請求項3記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに異なる第2のセッションキーを、さらに、第1の復号鍵により復号可能な暗号化を施して供給を受け、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに更新される第1のセッションキーを生成する第1のセッションキー発生部と、第1のセッションキーを、外部から入力されたデータから第1の複合鍵に基づいて第1の復号処理部にて抽出された第2のセッションキーで暗号化してデータ格納部に与えるための第2の暗号化処理部と、第1のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第1のセッションキーについて復号して第1の復号処理部に与える第3の復号処理部をさらに含む。

【0015】

請求項4記載のデータ再生装置は、請求項1～3のいずれか1項に記載のデータ再生装置の構成に加えて、コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、データ再生部は、符号化

音楽データから符号化方式に基づいて音楽データを再生する音楽再生部と、再生した音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む。

【0016】

請求項5記載のデータ再生装置は、請求項2記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記憶部と、第1の暗号化鍵を保持する第2の鍵保持部と、第1の暗号化鍵により暗号化されたデータを復号するための第2の復号鍵を保持するための第3の鍵保持部と、第2の復号鍵に基づいて、データ再生部から第1の暗号化鍵により暗号化されて伝達された第1のセッションキーを復号するための第4の復号処理部と、第4の復号処理部で抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第2の暗号化処理部を備える。

【0017】

請求項6記載のデータ再生装置は、請求項3記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記録部と、暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第2のセッションキーを発生する第2のセッションキー発生部と、第1の復号鍵にて復号可能な第2の暗号化鍵により、暗号化処理を行なう第3の暗号化処理部と、第2のセッションキーに基づいて、データ再生部から第2のセッションキーにて暗号化されて伝達された第1のセッションキーを復号するための第5の復号処理手段と、第5の復号処理手段にて抽出された第1のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第4の暗号化処理部を備える。

【0018】

請求項7記載のデータ再生装置は、請求項5または6記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【0019】

請求項8記載のデータ再生装置は、請求項1記載のデータ再生装置の構成に加

えて、データ再生部は、少なくとも第 1 の鍵保持部と、第 1 の復号処理部と、第 2 の復号処理部とが、第三者には読出不可能なセキュリティー領域に設けられている。

【0020】

請求項 9 記載のデータ再生装置は、請求項 1 ～ 4 のいずれか 1 項に記載のデータ再生装置の構成に加えて、データ再生部は、第三者には読出不可能なセキュリティー領域に設けられる。

【0021】

【発明の実施の形態】

【実施の形態 1】

【システムの全体構成】

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【0022】

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

【0023】

図 1 を参照して、著作権の存在する音楽情報を管理する配信サーバ 10 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリアである携帯電話会社 20 に、このような暗号化データを与える。

【0024】

携帯電話会社 20 は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ 10 に中継する。配信サーバ 10 は、配線リクエストがあると、要求された暗号化音楽情報を携帯電話会社 20 の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【0025】

さらに、たとえばユーザ1は、携帯電話100に接続したヘッドホン140等を介してこのような再生された音楽データを聴取することが可能である。

【0026】

以下では、このような配信サーバ10と配信キャリア（携帯電話会社）20とを併せて、音楽サーバ30と総称することにする。

【0027】

また、このような音楽サーバ30から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【0028】

しかも、配信キャリア20において、たとえば1曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0029】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0030】

〔配信サーバ10の構成〕

図1において配信サーバ10は、音楽データ（コンテンツデータ）を所定的方式に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース304と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース302と、暗号化コンテンツデータを復号するためのコンテンツキーK_cを公開暗号化キーK_{PP}により暗号化するためのコンテンツキー暗号化処理部316と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、配信サーバ10の動作を制御するためのコントローラ312と、通

信網を介して、配信サーバ 1 0 と配信キャリア 2 0 との間でデータ授受を行なうための通信装置 3 5 0 とを備える。

【 0 0 3 1 】

すなわち、配信情報データベース 3 0 4 からは、コンテンツデータ D_c が、共通暗号鍵であるコンテンツキー K_c により暗号化したデータ $[D_c] K_c$ と、コンテンツキー K_c とが出力される。コントローラ 3 1 2 は、コンテンツキー暗号化処理部 3 1 6 を制御して、このコンテンツキー K_c を公開暗号化キー K_P により暗号化した $[K_c] K_P$ を通信装置 3 5 0 を介して、配信キャリア 2 0 に与える。

【 0 0 3 2 】

ここで、 $[Y] X$ という表記は、データ Y を、鍵データ X により復号可能な暗号に変換した情報であることを示している。

【 0 0 3 3 】

〔端末（携帯電話機）の構成〕

図 2 は、図 1 に示した携帯電話 1 0 0 の構成を説明するための概略ブロック図である。

【 0 0 3 4 】

携帯電話 1 0 0 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1 1 0 2 と、アンテナ 1 1 0 2 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話からのデータを変調してアンテナ 1 1 0 2 に与えるための送受信部 1 1 0 4 と、携帯電話 1 0 0 の各部のデータ授受を行なうためのデータバス BS_2 と、データバス BS_2 を介して携帯電話 1 0 0 の動作を制御するためのコントローラ 1 1 0 6 と、外部からの指示を携帯電話 1 0 0 に与えるためのタッチキーやダイヤルキーなどを含むキーボード 1 1 0 8 と、コントローラ 1 1 0 6 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1 1 1 0 と、通常の通話動作において、データバス BS_2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1 1 1 2 とを備える。

【 0 0 3 5 】

携帯電話 1 0 0 は、さらに、サーバ 3 0 からの暗号化コンテンツデータ $[D_c$

】 K c および暗号化されたコンテンツキー [K c] K p を格納するためのメモリ 110 と、音楽再生モジュール 1500 とを備える。この音楽再生モジュール 1500 は、公開暗号化キー K P p に対応し、キー K P p で暗号化されたデータを復号可能な秘密復号キー K p を保持する K p 保持部 1540 と、音楽サーバ 30 から伝送され公開暗号化キー K P p により暗号化されたコンテンツキー [K c] K p をメモリ 110 から受けて復号するための復号処理部 1530 と、音楽サーバ 30 から配信されメモリ 110 中に格納された暗号化コンテンツデータ [D c] K c を、復号処理部 1530 で復号抽出されたコンテンツキー K c に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば MP3、AC3 等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

【0036】

携帯電話機 100 は、さらに、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 140 と接続するための接続端子 1514 とを含む。

【0037】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0038】

また、図 2 に示した構成において、音楽再生部 1508、K p 保持部 1540、復号処理部 1530 および復号処理部 1520 を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール T R M に組み込む構成とすることが可能である。このようなモジュールは、一般に

はタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【0039】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 100 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0040】

さらに、図 2 において実線で囲んだ領域に相当する音楽再生モジュール 150 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【0041】

〔再生処理〕

図 3 は、携帯電話 100 内において、メモリ 110 に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0042】

図 3 を参照して、携帯電話のキーボード 1108 等からのユーザの指示により、再生リクエストがコントローラ 1106 に与えられる (ステップ S100)。

【0043】

この再生リクエストに応じて、コントローラ 1106 は、メモリ 110 を制御して暗号化されたコンテンツキー [Kc] Kp を読み出す (ステップ S102)

。

【0044】

つづいて、復号処理部 1530 は、メモリ 110 から読み出された暗号化されたコンテンツキー [Kc] Kp に対する復号処理を行なう (ステップ S104)

。

【0045】

復号処理部 1530 においてコンテンツキー Kc を復号抽出可能な場合は、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了す

る（ステップ S110）。

【0046】

復号処理部 1530 においてコンテンツキー Kc を復号抽出可能な場合は、コントローラ 1108 は、メモリ 110 を制御して、暗号化コンテンツデータ [Dc] Kc を読み出して、復号処理部 1520 に与え、復号処理部 1520 は、復号キー Kc により復号処理して、平文化したコンテンツデータ Dc を生成して音楽再生部 1508 に与える。音楽再生部 1508 により再生された音楽信号は、混合部 1510 を経由して、デジタルアナログ変換器 1512 によりアナログ信号に変換されて接続端子 1514 から外部に出力される。

【0047】

以上のような構成とすることで、再生装置である携帯電話機 100 内のメモリ 110 には、暗号化されたコンテンツデータと暗号化されたコンテンツキーが保持されているのみであるため、外部からこのメモリ 110 内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

【0048】

しかも、メモリ 110 から復号処理部 1520 および 1530 に与えられるデータも、このような暗号化されたデータであるため、データバス BS2 上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

【0049】

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパージェスタンスモジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

【0050】

したがって、図 2 に示した携帯電話機 100 の構成により、ユーザ以外の者が無断でコンテンツデータに対してアクセスを行なうことから保護することが可能となる。

【0051】

〔実施の形態 2〕

図 4 は、本発明の実施の形態 2 の携帯電話機 200 の構成を説明するための概

略ブロック図であり、実施の形態 1 の図 2 と対比される図である。

【0052】

図 2 に示した携帯電話機 100 の構成と、携帯電話機 200 の構成が異なる点は、以下のとおりである。

【0053】

まず、図 4 においては、携帯電話機 200 には、携帯電話機 200 により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機 200 中の音楽再生モジュール 1500 に与えるための着脱可能なメモリカード 120 が装着される構成となっている。これに応じて、携帯電話機 200 は、メモリカード 120 とデータバス BS2 との間のデータの授受を制御するためのメモリインタフェース 1200 をさらに備えている。

【0054】

さらに、携帯電話機 200 の構成では、音楽再生モジュール 1500 の構成も、携帯電話機 100 の構成と異なる。

【0055】

すなわち、携帯電話機 200 の音楽再生モジュール 1500 は、メモリカード 120 と携帯電話の他の部分とのデータ授受にあたり、データバス BS2 上においてやり取りされるデータを暗号化するための後に説明するセッションキー Ks を乱数等により発生するセッションキー発生部 1502 と、セッションキー発生部 1502 により生成されたセッションキー Ks を暗号化して、データバス BS2 に与えるための暗号化処理部 1504 と、データバス BS2 によりメモリカード 120 から伝送され、公開暗号鍵 K P p およびセッションキー Ks により暗号化されたコンテンツキーをセッションキー Ks について復号して出力する復号処理部 1506 と、公開暗号化キー K P p に対応し、キー K P p で暗号化されたデータを復号可能な秘密復号キー K p を保持する K p 保持部 1540 と、復号処理部 1506 の出力を受けて、メモリカード 120 から伝送され公開暗号化キー K P p により暗号化されたコンテンツキー [K c] K p を復号するための復号処理部 1530 と、サーバ 30 から配信されメモリカード 120 中に格納された暗号

化コンテンツデータ [Dc] Kc を、復号処理部 1530 で復号抽出されたコンテンツキー Kc に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータ Dc を受けて、音楽サーバ 30 から配信された音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

【0056】

携帯電話機 200 のその他の部分は、実施の形態 1 の携帯電話機 100 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0057】

なお、図 4 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0058】

また、図 4 に示した構成において、音楽再生部 1508、Kp 保持部 1540、復号処理部 1530、復号処理部 1520、復号処理部 1506、暗号化処理部 1504 および Ks 発生部 1502 を、TRM に組み込む構成とすることが可能である。

【0059】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 200 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0060】

さらに、図 4 において実線で囲んだ領域に相当する音楽再生モジュール 1500 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【 0 0 6 1 】

〔暗号／復号キーの構成〕

図 5 は、図 4 に示した携帯電話機 2 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【 0 0 6 2 】

まず、図 4 に示した構成において、メモ리카ード 1 2 0 内のデータ処理を管理するための鍵としては、メモ리카ードに固有な公開暗号化鍵 $K P m$ と、公開暗号化鍵 $K P m$ により暗号化されたデータを復号するためのキー $K P m$ とは非対称な秘密復号鍵 $K m$ とがある。

【 0 0 6 3 】

ここで、キー $K P m$ とキー $K m$ とが非対称とは、複数の公開暗号化キー $K P m$ により暗号化されたデータが同一の復号キー $K m$ により復号できることを意味する。

【 0 0 6 4 】

したがって、メモ리카ード 1 2 0 と携帯電話 2 0 0 とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵 $K m$ 、復号鍵 $K P m$ が用いられることになる。

【 0 0 6 5 】

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化キーを $K P p$ と、音楽再生モジュール管理の鍵として、このキー $K P p$ で暗号化されたデータを復号化でき、キー $K P p$ とは非対称な秘密復号キー $K p$ と、各通信ごとに $K s$ 発生器 1 5 0 2 において生成される共通鍵 $K s$ とが用いられる。

【 0 0 6 6 】

ここで、共通鍵 $K s$ は、たとえば、携帯電話機 2 0 0 とメモ리카ード 1 2 0 との間のコンテンツデータの授受のためのアクセスが行なわれるごとに $K s$ 発生器 1 5 0 2 において発生する。

【 0 0 6 7 】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と

呼ぶことにし、共通鍵 K_s を「セッションキー」とも呼ぶことにする。

【0068】

したがって、共通鍵 K_s は各通信セッションに固有の値を有することになり、音楽再生モジュール 1500 において管理される。

【0069】

さらに、メモ리카ード 120 に記録される著作権情報データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキー K_c があり、この共通鍵 K_c により暗号化されたコンテンツデータが復号（平文化）されるものとする。

【0070】

著作権の存在するコンテンツデータ D_c は、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキー K_c で復号化可能なデータを、暗号化コンテンツデータ $[D_c] K_c$ と呼ぶ。

【0071】

また、配信サーバ 10 から携帯電話機 200 に向けて、コンテンツキー K_c が配信される場合には、このコンテンツキー K_c は、すくなくとも公開暗号化キー K_Pp により暗号化されており、メモ리카ード 120 中には、この暗号化コンテンツキー $[K_c] K_Pp$ として格納されているものとする。

【0072】

〔メモ리카ードの構成〕

図 6 は、図 4 に示したメモ리카ード 120 の構成を説明するための概略ブロック図である。

【0073】

メモ리카ード 120 は、メモリアインタフェース 1200 との間で信号を端子 1202 を介して授受するデータバス $BS3$ と、公開暗号化キー K_Pm の値を保持し、データバス $BS3$ に公開暗号化キー K_Pm を出力するための K_Pm 保持部 1401 と、カード 120 に対応する秘密復号鍵 K_m を保持するための K_m 保持部 1402 と、データバス $BS3$ にメモリアインタフェース 1200 から与えられるデータから、秘密復号鍵 K_m により復号処理をすることにより、セッションキー

K_sを抽出する復号処理部1404と、データバスBS3から、公開暗号化キーK_pで暗号化されているコンテンツキーK_cおよびコンテンツキーK_cにより暗号化されている暗号化コンテンツデータ[D_c]K_cを受けて格納するためのメモリ1412と、復号処理部1404により抽出されたセッションキーK_sに基づいて、メモリ1412からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1406と、メモリカード120の動作を制御するためのコントローラ1420とを備える。

【0074】

なお、図6のメモリカード120内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

【0075】

〔再生処理〕

図7は、携帯電話機200内において、メモリカード120に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0076】

図7を参照して、携帯電話のキーボード1108等からのユーザの指示により、再生リクエストがメモリカード120に対して出力される（ステップS200）。

【0077】

メモリカード120においては、この再生リクエストに応じて、コントローラ1420は、K_{Pm}保持部1401から、データバスBS3、端子1202およびメモリインターフェース1200を介して、公開暗号化キーK_{Pm}を携帯電話200に対して送信する（ステップS202）。

【0078】

携帯電話機200では、カード120からのキーK_{Pm}を受信すると（ステップS204）、K_s発生部1502においてセッションキーK_sを生成し（ステ

ップS206)、暗号化処理部1504が、キーK_{Pm}により、セッションキーK_sを暗号化してデータ[K_s]K_{Pm}を生成し、データバスBS2を介して、カード120に対して送信する(ステップS208)。

【0079】

メモリカード120は、携帯電話機200により生成され、かつ暗号化されたセッションキーK_sを受け取り、復号処理部1404において秘密復号キーK_mにより復号し、セッションキーK_sを抽出する(ステップS210)。

【0080】

続いて、メモリカード120は、メモリ1412から、暗号化されているデータ[K_c]K_pを読出す(ステップS212)。

【0081】

続いて、メモリカード120は、暗号化処理部1406において抽出したセッションキーK_sにより、暗号化コンテンツキー[K_c]K_pを暗号化し、暗号化された暗号化コンテンツキー[[K_c]K_p]K_sをデータバスBS2に与える(ステップS214)。

【0082】

携帯電話機200の復号処理部1506は、メモリカード120から送信された暗号化された暗号化コンテンツキー[[K_c]K_p]K_sをセッションキーK_sにより復号処理を行なうことにより、暗号化コンテンツキー[K_c]K_pを取得する(ステップS216)。

【0083】

さらに、携帯電話機200の復号処理部1530は、K_p保持部1540からのキーK_pに基づいて、データ[K_c]K_pの復号処理を行なう(ステップS218)。

【0084】

復号処理部1530が復号処理により、コンテンツキーK_cを抽出できた場合は(ステップS220)、処理は次のステップS222に進み、抽出できない場合は(ステップS220)、処理は終了する(ステップS226)。

【0085】

復号処理部 1 5 3 0 が復号処理により、コンテンツキー K c を抽出できた場合は、メモリカード 1 2 0 は、暗号化されたコンテンツデータ [D c] K c をメモリ 1 4 1 2 から読出し、データバス B S 2 に与える（ステップ S 2 2 2）。

【0 0 8 6】

携帯電話機 2 0 0 の復号処理部 1 5 2 0 は、暗号化されたコンテンツデータ [D c] K c を、抽出されたコンテンツキー K c により復号処理して平文の音楽データ D c を生成し、音楽再生部 1 5 0 8 は、コンテンツデータ D c を再生して混合部 1 5 1 0 に与える。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 2 6）。

【0 0 8 7】

このような構成とすることで、携帯電話機 2 0 0 において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード 1 2 0 から携帯電話機 2 0 0 に送信して再生動作を行なうことが可能となる。

【0 0 8 8】

以上のような構成により、実施の形態 1 の携帯電話機 1 0 0 の奏する効果に加えて、実施の形態 2 の携帯電話機 2 0 0 においては、携帯電話機 2 0 0 に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

【0 0 8 9】

しかも、携帯電話機とメモリカードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれるので、データに対するセキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【0 0 9 0】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【0 0 9 1】

〔実施の形態 3〕

図 8 は、本発明の実施の形態 3 の携帯電話機 3 0 0 の構成を説明するための概略ブロック図であり、実施の形態 2 の図 4 と対比される図である。

【0 0 9 2】

図 8 に示した実施の形態 3 の携帯電話機 3 0 0 の構成と、実施の形態 2 の携帯電話機 2 0 0 の構成が異なる点は、以下のとおりである。

【0 0 9 3】

まず、図 8 においては、携帯電話機 3 0 0 には、携帯電話機 3 0 0 により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機 3 0 0 中の音楽再生モジュール 1 5 0 0 に与えるための着脱可能なメモリカード 1 3 0 が装着される構成となっている。

【0 0 9 4】

メモリカード 1 3 0 は、後に説明するように、メモリカード 1 3 0 自身でセッションキー K s 2 を生成する点で、メモリカード 1 2 0 と異なる。

【0 0 9 5】

さらに、携帯電話機 3 0 0 の構成では、音楽再生モジュール 1 5 0 0 の構成も、携帯電話機 2 0 0 の構成と異なる。

【0 0 9 6】

すなわち、携帯電話機 3 0 0 の音楽再生モジュール 1 5 0 0 は、メモリカード 1 3 0 と携帯電話の他の部分とのデータ授受にあたり、データバス B S 2 上においてやり取りされるデータを暗号化するためのセッションキー K s 1 を乱数等により発生するセッションキー発生部 1 5 5 2 と、セッションキー発生部 1 5 5 2 により生成されたセッションキー K s 1 をメモリカード 1 3 0 からのセッションキー K s 2 で暗号化して、データバス B S 2 に与えるための暗号化処理部 1 5 5 4 と、データバス B S 2 によりメモリカード 1 3 0 から伝送され、公開暗号鍵 K P p およびセッションキー K s 1 により暗号化されたコンテンツキー K c をセッションキー K s 1 について復号して出力する復号処理部 1 5 5 6 と、コントローラ 1 1 0 6 により制御されて、データバス B S 2 により伝達された暗号化された

メモリカード 130 のセッションキー [Ks2] Kp または復号処理部 1556 から出力された暗号化コンテンツキー [Kc] Kp のいずれかを、公開暗号化鍵 KPp により暗号化されたデータを復号するための復号処理部 1530 に与える切換え回路 1550 とを含む。

【0097】

暗号化処理部 1554 は、復号処理部 1530 において秘密復号鍵 Kp により復号されて抽出されたメモリカード 130 のセッションキー Ks2 を受けて、セッションキー発生部 1552 により生成されたセッションキー Ks1 をセッションキー Ks2 で暗号化処理する。

【0098】

携帯電話機 300 のその他の部分は、実施の形態 2 の携帯電話機 200 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0099】

なお、図 8 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0100】

また、図 8 に示した構成において、音楽再生部 1508、Kp 保持部 1540、復号処理部 1530、復号処理部 1520、復号処理部 1556、暗号化処理部 1554、セッションキー発生部 1552 および切換え回路 1550 を、TRM に組み込む構成とすることが可能である。

【0101】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機 300 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【0102】

さらに、図 8 において実線で囲んだ領域に相当する音楽再生モジュール 1500 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが

可能である。

【0 1 0 3】

〔暗号／復号キーの構成〕

図 9 は、図 8 に示した携帯電話機 3 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0 1 0 4】

まず、図 8 に示した構成において、メモ리카ード 1 3 0 内のデータ処理を管理するための鍵としては、メモ리카ードに固有な公開暗号化鍵 $K P_m$ と、公開暗号化鍵 $K P_m$ により暗号化されたデータを復号するためのキー $K P_m$ とは非対称な秘密復号鍵 K_m と、メモ리카ード 1 3 0 が生成し各セッションに固有なセッションキー $K s_2$ とがある。

【0 1 0 5】

したがって、メモ리카ード 1 3 0 と携帯電話 3 0 0 とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵 K_m 、復号鍵 $K P_m$ 、セッションキー $K s_2$ が用いられることになる。

【0 1 0 6】

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化キーであって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモ리카ード 1 3 0 内に記憶される公開暗号鍵 $K P_p$ と、音楽再生モジュールの管理の鍵として、このキー $K P_p$ で暗号化されたデータを復号化でき、キー $K P_p$ とは非対称な秘密復号キー K_p と、各アクセスごとにセッションキー発生器 1 5 5 2 において生成される共通鍵（セッションキー） $K s_1$ とが用いられる。

【0 1 0 7】

共通鍵 $K s_1$ も各通信セッションに固有の値を有することになり、音楽再生モジュール 1 5 0 0 において管理される。

【0 1 0 8】

さらに、メモ리카ード 1 3 0 に記録される著作権情報データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテ

ンツキー K_c があり、この共通鍵 K_c により暗号化されたコンテンツデータが復号（平文化）されるものとする。

【0109】

また、配信サーバ 10 から携帯電話機 300 に向けて、コンテンツキー K_c が配信される場合には、このコンテンツキー K_c は、すくなくとも公開暗号化キー K_{Pp} により暗号化されており、メモリカード 120 中には、この暗号化コンテンツキー [K_c] K_p として格納されているものとする。

【0110】

さらに、著作権の存在するコンテンツデータ D_c は、このコンテンツデータをコンテンツキー K_c で復号化可能な暗号化コンテンツデータ [D_c] K_c としてメモリカード 130 に格納されているものとする。

【0111】

〔メモリカードの構成〕

図 10 は、図 8 に示したメモリカード 130 の構成を説明するための概略ブロック図である。

【0112】

メモリカード 130 は、メモリインタフェース 1200 との間で信号を端子 1202 を介して授受するデータバス B_{S3} と、セッション毎にセッションキー K_{s2} を生成するためのセッションキー発生部 1450 と、セッションキー K_{s2} を公開暗号化鍵 K_{Pp} で暗号化してデータバス B_{S3} に与えるための暗号化処理部 1452 と、データバス B_{S3} にメモリインタフェース 1200 から与えられるデータ [K_{s1}] K_{s2} から、セッションキー K_{s2} により復号処理をすることにより、携帯電話機 300 からのセッションキー K_{s1} を抽出する復号処理部 1454 と、データバス B_{S3} から、公開暗号化鍵 K_{Pp} と公開暗号化鍵 K_{Pp} で暗号化されているコンテンツキー [K_c] K_p とコンテンツキー K_c により暗号化されている暗号化コンテンツデータ [D_c] K_c との 3 つを受けて格納するためのメモリ 1412 と、復号処理部 1454 により抽出されたセッションキー K_{s1} に基づいて、メモリ 1412 からの出力を暗号化してデータバス B_{S3} に与えるための暗号化処理部 1456 と、メモリカード 130 の動作を制御するた

めのコントローラ 1 4 2 0 とを備える。

【0 1 1 3】

なお、図 1 0 のメモリカード 1 3 0 内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール T R M に組込まれる構成とすることも可能である。

【0 1 1 4】

〔再生処理〕

図 1 1 は、携帯電話機 3 0 0 内において、メモリカード 1 3 0 に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0 1 1 5】

図 1 1 を参照して、携帯電話のキーボード 1 1 0 8 等からのユーザの指示により、再生リクエストがメモリカード 1 3 0 に対して出力される（ステップ S 3 0 0）。

【0 1 1 6】

メモリカード 1 3 0 においては、この再生リクエストに応じて、コントローラ 1 4 2 0 は、セッションキー発生部 1 4 5 0 を制御してセッションキー K s 2 を発生させる（ステップ S 3 0 2）。コントローラ 1 4 2 0 の制御により、このセッションキー K s 2 を暗号化処理部 1 4 5 2 は公開暗号化鍵 K P p により暗号化して暗号化セッションキー [K s 2] K p を生成し、この暗号化セッションキー [K s 2] K p を、データバス B S 3、端子 1 2 0 2 およびメモリインターフェース 1 2 0 0 を介して、携帯電話 3 0 0 に対して送信する（ステップ S 3 0 4）。

【0 1 1 7】

携帯電話機 3 0 0 では、カード 1 3 0 からの暗号化セッションキー [K s 2] K p を受信すると、切換え回路 1 5 5 0 を介して復号処理部 1 5 3 0 が暗号化セッションキー [K s 2] K p を受けて復号しセッションキー K s 2 を獲得する（ステップ S 3 0 6）。

【0118】

携帯電話機300においては、セッションキー発生部1552においてセッションキー $Ks1$ を生成し（ステップS308）、暗号化処理部1554が、ステップS306において抽出されたセッションキー $Ks2$ により、セッションキー $Ks1$ を暗号化してデータ $[Ks1]Ks2$ を生成し、データバスBS2を介して、カード130に対して送信する（ステップS310）。

【0119】

メモリカード130は、携帯電話機300により生成され、かつ暗号化されたセッションキー $[Ks1]Ks2$ を受け取り、復号処理部1454においてセッションキー $Ks2$ により復号し、セッションキー $Ks1$ を抽出する（ステップS312）。

【0120】

続いて、メモリカード130は、メモリ1412から、暗号化されているデータ $[Kc]Kp$ を読出す（ステップS314）。

【0121】

続いて、メモリカード130は、暗号化処理部1456において、抽出したセッションキー $Ks1$ により、暗号化コンテンツキー $[Kc]Kp$ を暗号化し、暗号化された暗号化コンテンツキー $[[Kc]Kp]Ks1$ をデータバスBS3等を介してデータバスBS2に与える（ステップS316）。

【0122】

携帯電話機300の復号処理部1556は、メモリカード130から送信された暗号化された暗号化コンテンツキー $[[Kc]Kp]Ks1$ に対してセッションキー $Ks1$ により復号処理を行なうことにより、暗号化コンテンツキー $[Kc]Kp$ を取得する（ステップS318）。

【0123】

さらに、携帯電話機300の復号処理部1530は、切換え回路1550を介して暗号化コンテンツキー $[Kc]Kp$ を受け、 Kp 保持部1540からのキー Kp に基づいて、データ $[Kc]Kp$ の復号処理を行なう（ステップS320）。

。

【0 1 2 4】

復号処理部 1 5 3 0 が復号処理により、コンテンツキー K c を抽出できた場合は（ステップ S 3 2 2）、処理は次のステップ S 3 2 4 に進み、抽出できない場合は（ステップ S 3 2 2）、処理は終了する（ステップ S 3 3 0）。

【0 1 2 5】

復号処理部 1 5 3 0 が復号処理により、コンテンツキー K c を抽出できた場合は、メモリカード 1 3 0 は、暗号化されたコンテンツデータ [D c] K c をメモリ 1 4 1 2 から読出し、データバス B S 3 等を介してデータバス B S 2 に与える（ステップ S 3 2 4）。

【0 1 2 6】

携帯電話機 3 0 0 の復号処理部 1 5 2 0 は、暗号化されたコンテンツデータ [D c] K c を、抽出されたコンテンツキー K c により復号処理して平文の音楽データ D c を生成し、音楽再生部 1 5 0 8 は、コンテンツデータ D c を再生して混合部 1 5 1 0 に与える。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップ S 3 2 8）、処理が終了する（ステップ S 3 3 0）。

【0 1 2 7】

このような構成とすることで、携帯電話機 3 0 0 において生成されたセッションキー K s 1 に基づいてコンテンツキーを暗号化した上で、メモリカード 1 3 0 から携帯電話機 3 0 0 に送信して再生動作を行なうことが可能となる。しかも、メモリカード 1 3 0 においてセッション毎に生成されたセッションキー K s 2 により暗号化した上で、メモリカード 1 3 0 と携帯電話 3 0 0 との間でセッションキー K s 1 の授受が行なわれるので、実施の形態 2 よりも一層、セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【0 1 2 8】

また、以上のような構成により、実施の形態 3 の形携帯電話機 3 0 0 においても、携帯電話機 3 0 0 に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれる

ことがない。

【0 1 2 9】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【0 1 3 0】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0 1 3 1】

【発明の効果】

以上説明したとおり、本願発明にかかるデータ再生装置では、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

【図面の簡単な説明】

【図 1】 本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図 2】 図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【図 3】 携帯電話機 1 0 0 内において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

【図 4】 本発明の実施の形態 2 の携帯電話機 2 0 0 の構成を説明するための概略ブロック図である。

【図 5】 図 4 に示した携帯電話機 2 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 6】 図 4 に示したメモリカード 1 2 0 の構成を説明するための概略ブ

ロック図である。

【図 7】 携帯電話機 2 0 0 内において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

【図 8】 本発明の実施の形態 3 の携帯電話機 3 0 0 の構成を説明するための概略ブロック図である。

【図 9】 図 8 に示した携帯電話機 3 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 1 0】 図 8 に示したメモリカード 1 3 0 の構成を説明するための概略ブロック図である。

【図 1 1】 携帯電話機 3 0 0 内において、暗号化コンテンツデータから音楽情報を復号化するための再生処理を説明するフローチャートである。

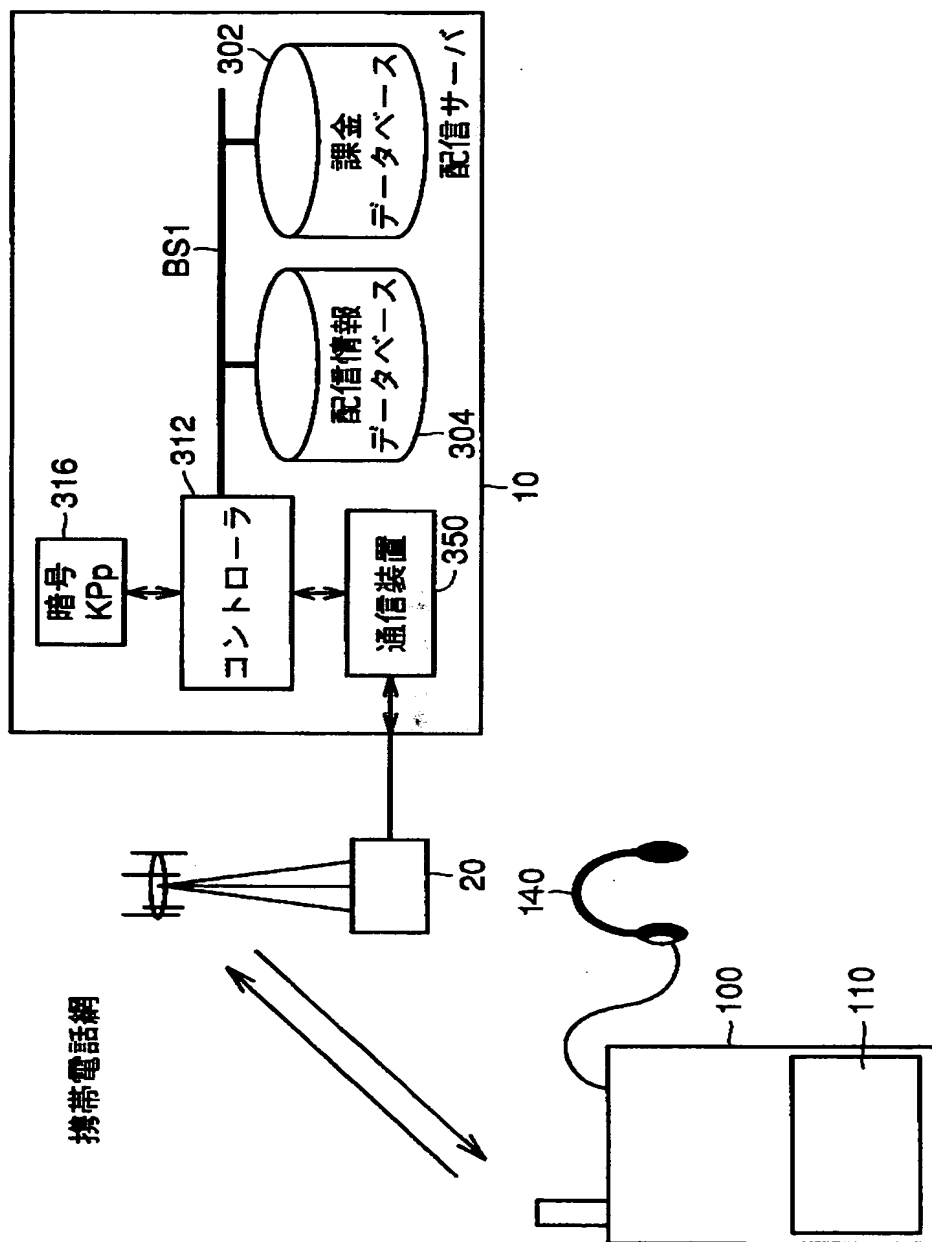
【符号の説明】

1 0 配信サーバ、2 0 配信キャリア、3 0 音楽サーバ、1 0 0, 2 0 0 携帯電話機、1 1 0, 1 2 0, 1 3 0 メモリカード、1 4 0 ヘッドホン、1 1 0 2 アンテナ、1 1 0 4 送受信機、1 1 0 6 コントローラ、1 1 0 8 キーボード、1 1 1 0 ディスプレイ、1 1 1 2 音声再生部、1 2 0 0 メモリインタフェース、1 4 0 1 K P m 保持部、1 4 0 4 復号処理部、1 4 0 6 暗号化処理部、1 4 2 0 コントローラ、1 5 0 2 セッションキー発生部、1 5 0 4 暗号化処理部、1 5 0 6 復号処理部、1 5 0 8 音楽再生部、1 5 1 0 混合部、1 5 1 2 デジタルアナログ変換器。

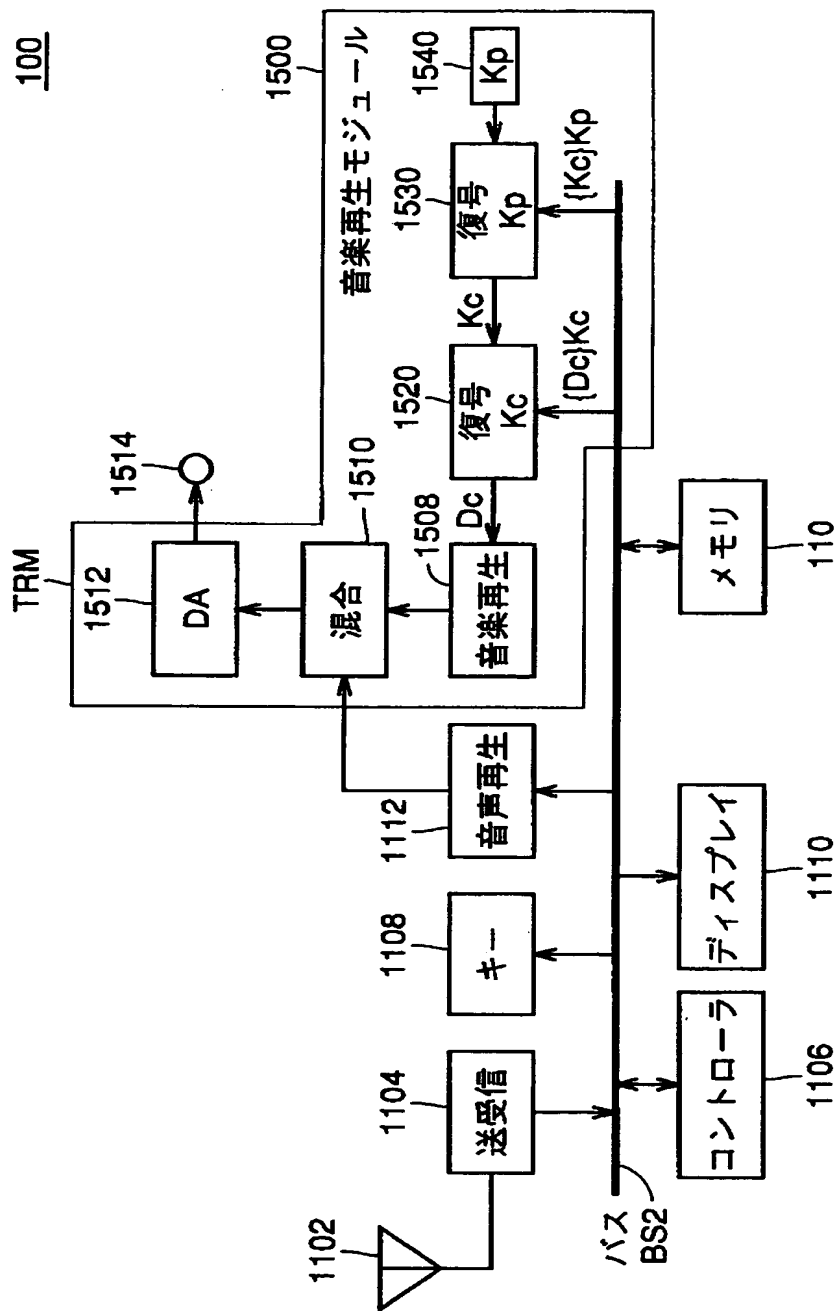
【書類名】

図面

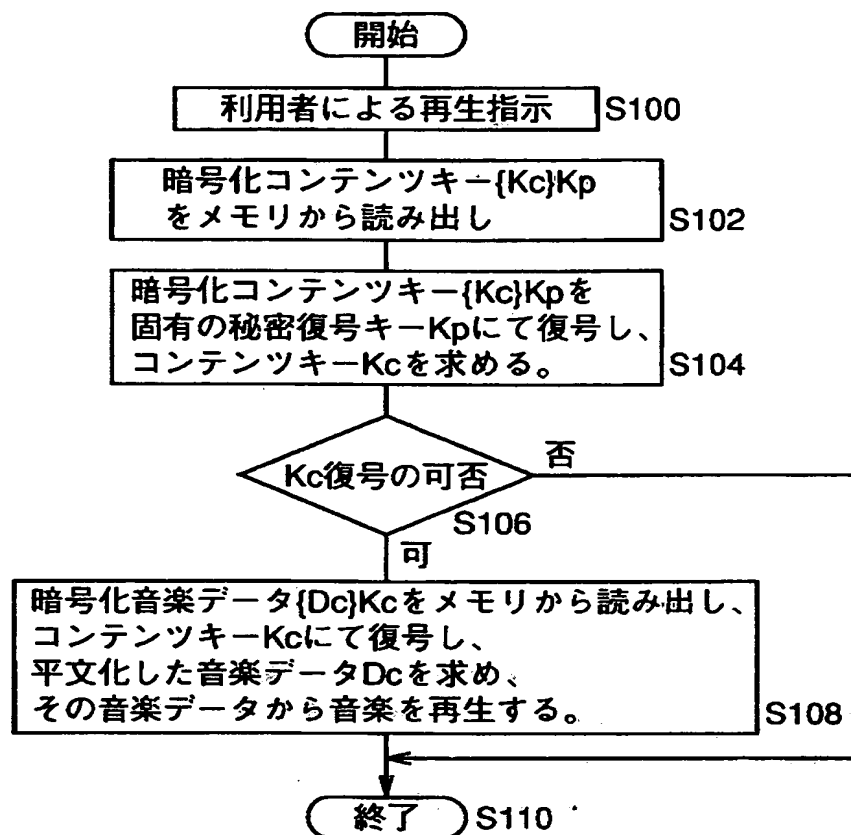
【図 1】



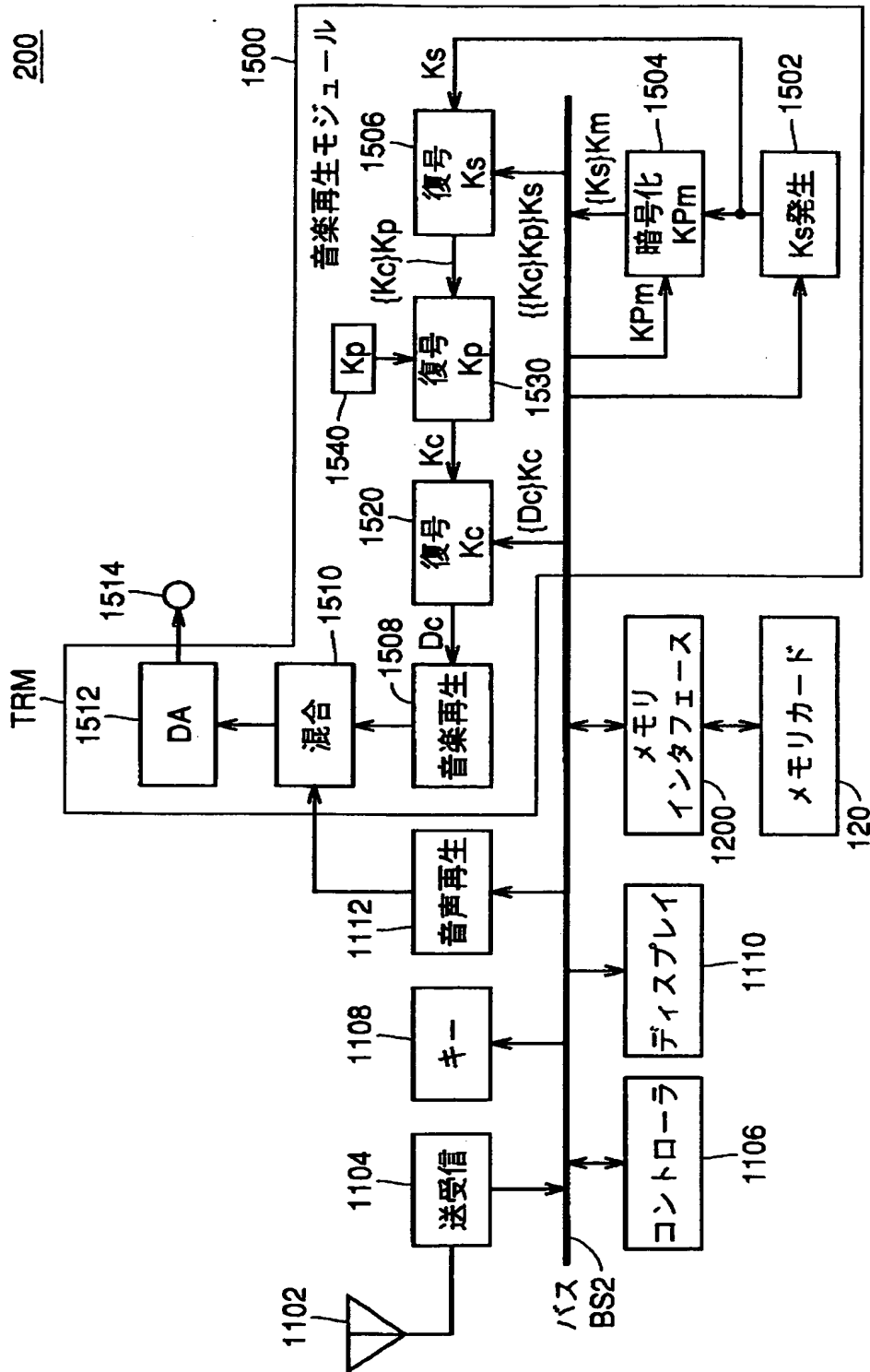
【図 2】



【図 3】



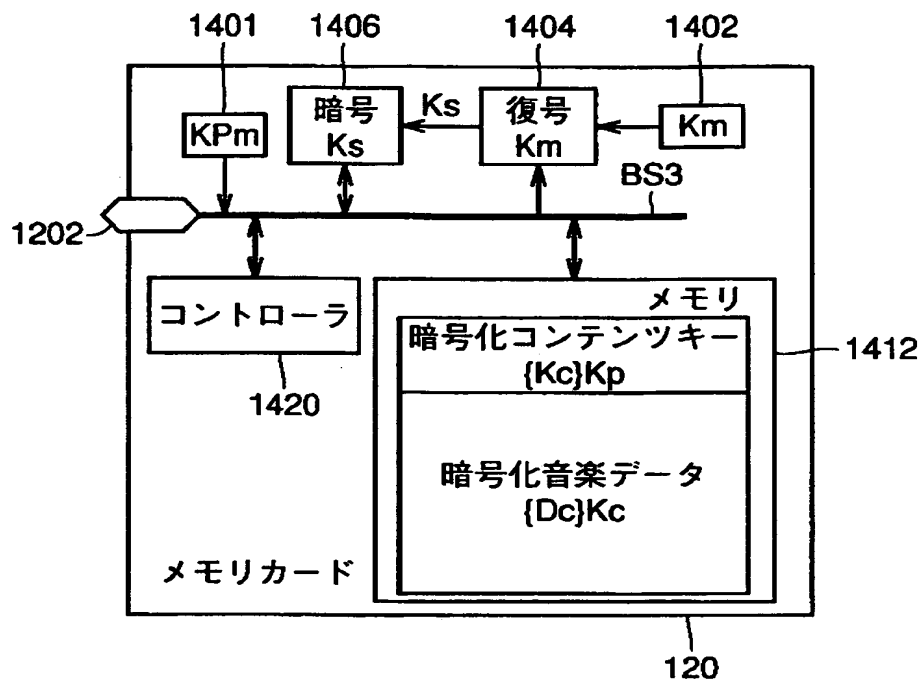
【図 4】



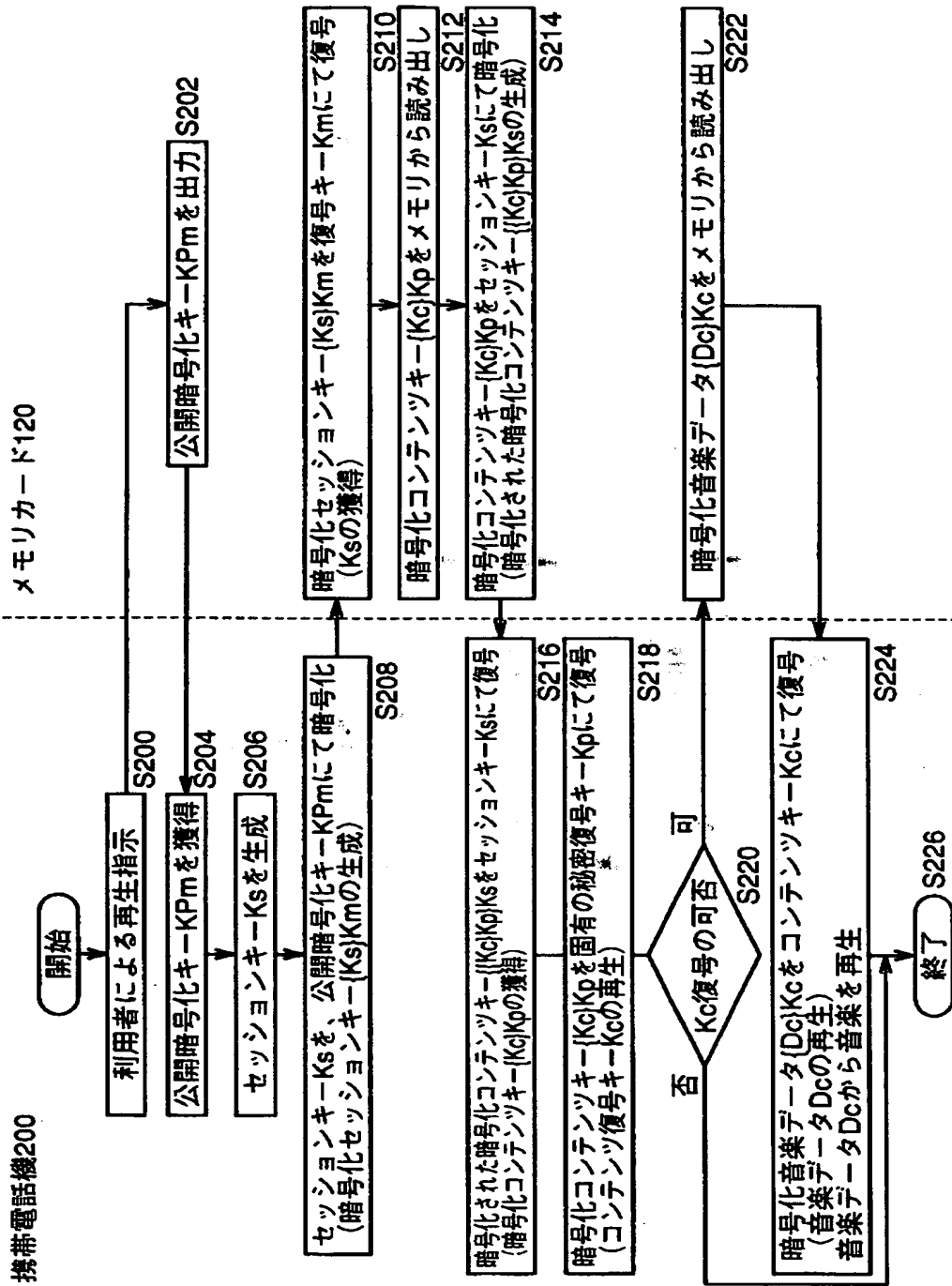
【図 5】

	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
音楽再生モジュール 管理の鍵	Kp	秘密復号鍵	データ再生装置毎に異なる
	Ks	共通鍵	データ再生装置 (携帯電話機) 固有 セッション固有
配信データ	KPp	公開暗号鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
	Kc	共通鍵	暗号化コンテンツデータの復号鍵
	Dc	コンテンツ データ	例：音楽データ

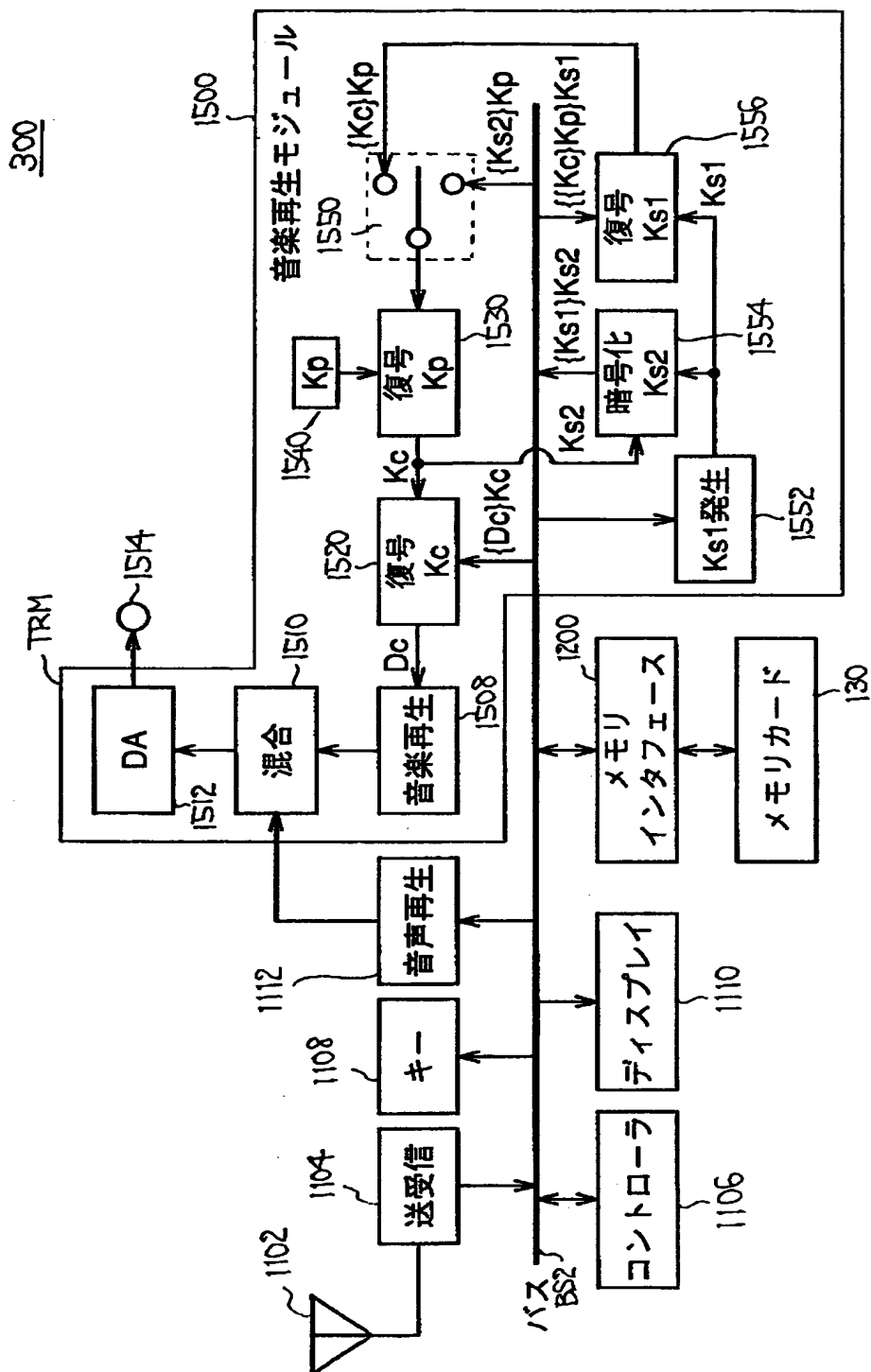
【図 6】



【図 7】



【图 8】

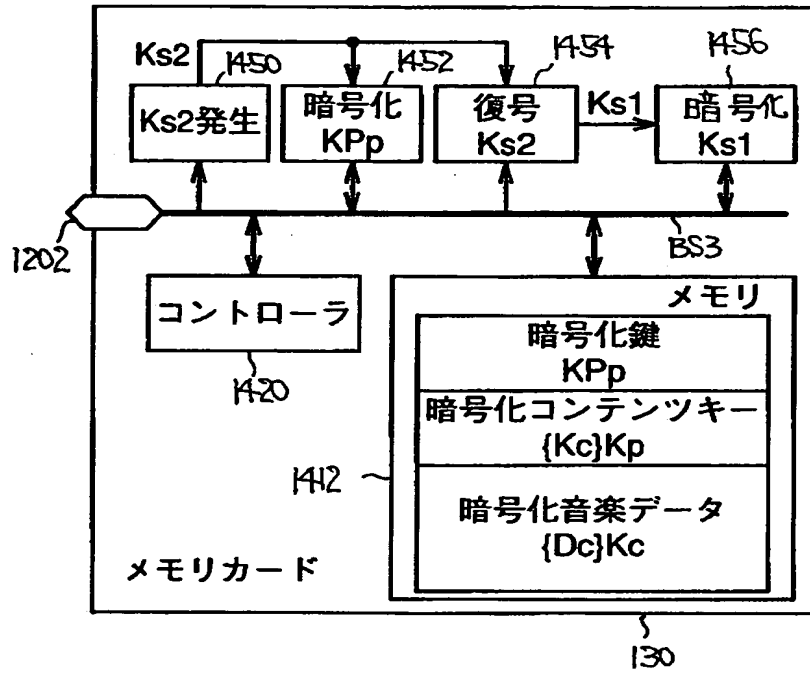


【図 9】

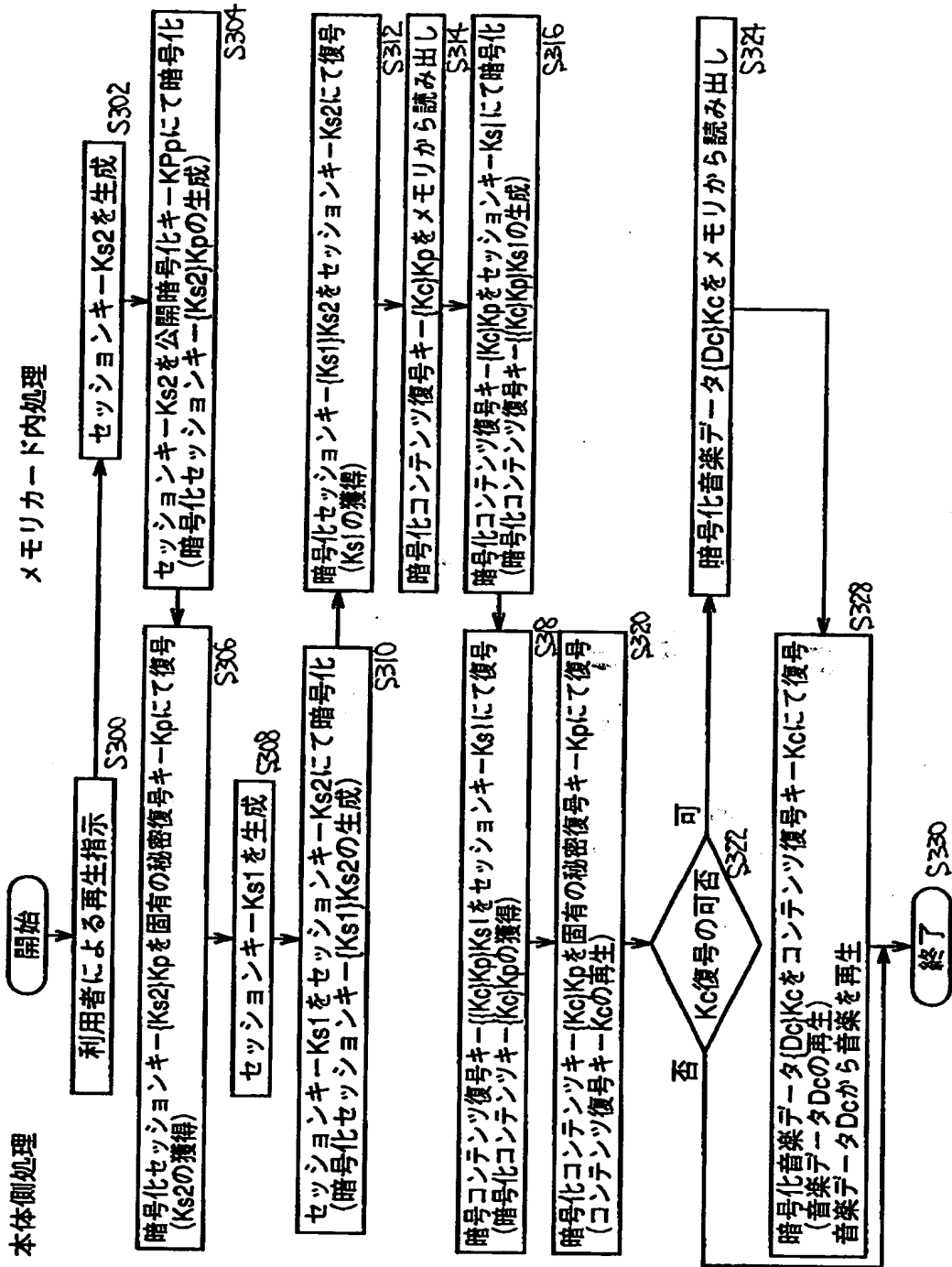
	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
	Ks2	共通鍵	メモリと音楽再生モジュール間 のアクセス毎に発生
	Kp	秘密復号鍵	データ再生装置毎に異なる (携帯電話機) 固有
音楽再生モジュール 管理の鍵	Ks1	共通鍵	メモリと音楽再生モジュール間 のアクセス毎に発生
	KPp	公開暗号鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
配信データ	Kc	共通鍵	暗号化コンテンツデータの復号鍵
	Dc	コンテンツ データ	例：音楽データ

【図 1 0】

メモリカード内の構造



【図 1 1】



【書類名】 要約書

【要約】

【課題】 許可なく著作権物情報データにアクセスされることを防止することが可能なデータ再生装置を提供する。

【解決手段】 携帯電話機 1 0 0 は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ 1 1 0 に格納する。メモリ 1 1 0 から読み出された暗号化コンテンツキーデータは、K_p 保持部 1 5 4 0 の保持するキーデータ K_p により復号処理部 1 5 3 0 により復号されて、音楽再生モジュール 1 5 0 0 に取り込まれる。復号処理部 1 5 2 0 は、メモリ 1 1 0 から読み出した暗号化コンテンツデータを、復号処理部 1 5 3 0 により抽出されたコンテンツキー K_c により復号して、コンテンツデータ D_c を再生する。

【選択図】 図 2

認定・付加情報

特許出願の番号	平成 11 年 特許願 第 243583 号
受付番号	59900838432
書類名	特許願
担当官	坪 政光 8844
作成日	平成 11 年 9 月 3 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂 4 丁目 14 番 14 号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通 2 丁目 5 番 5 号
【氏名又は名称】	三洋電機株式会社

【代理人】

申請人	
【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 29 号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 29 号 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
【住所又は居所】	大阪府大阪市北区南森町 2-1-29 住友銀行南森町ビル 深見特許事務所
【氏名又は名称】	伊藤 英彦

【選任した代理人】

次頁有

認定・付加情報（続き）

【識別番号】	100096781
【住所又は居所】	大阪府大阪市北区南森町 2 - 1 - 2 9 住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	堀井 豊

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社

出 願 人 履 歴 情 報

識別番号

[000004167]

1. 変更年月日

1990年 8月21日

[変更理由]

新規登録

住 所

東京都港区赤坂4丁目14番14号

氏 名

日本コロムビア株式会社

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日	1993年10月20日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通2丁目5番5号
氏 名	三洋電機株式会社